

**CLAIMS**

What is claimed is:

- 1 1. A computer-implemented method for controlling access by a plurality of client  
2 applications to file data in a distributed file system including a distributed file system  
3 interface coupled to the client applications and a storage server and a meta-data server  
4 coupled to the distributed file system interface, comprising:  
5 receiving at the meta-data server an open-file request, the open-file request  
6 specifying a name of a first file, wherein the first file includes a first set of blocks;  
7 creating a security object at the meta-data server in response to the open-file  
8 request;  
9 generating an encryption key at the meta-data server and the storage server and  
10 storing the encryption key in the security object;  
11 encrypting a list that identifies the first set of blocks, whereby an encrypted  
12 block list is formed;  
13 adding the encrypted block list to the security object; and  
14 transmitting the security object to the distributed file interface.
- 1 2. The method of claim 1, further comprising:  
2 transmitting a file access request and security object from the distributed file  
3 system interface to the storage server in response to a file access request from a client  
4 application, the file access request including an operation code and a reference to  
5 selected data of a file;  
6 decrypting the block list at the storage server in response to the file access  
7 request;  
8 providing access to the selected data in accordance with the operation code  
9 upon successful decryption of the block list.
- 1 3. The method of claim 2, further comprising:  
2 encrypting file data at the distributed file interface for file write operations using  
3 the encryption key in the security object; and  
4 decrypting file data at the distributed file interface for file read operations using  
5 the encryption key in the security object.

1 4. The method of claim 3, further comprising:  
2 generating a partial encryption key at the meta-data server and storing the  
3 partial encryption key in the security object;  
4 transmitting the security object to the storage server; and  
5 completing generation of the encryption key at the storage server using the  
6 partial encryption key and storing a complete encryption key in the security object; and  
7 returning the security object with the complete encryption key to the meta-data  
8 server.

1 5. The method of claim 4, further comprising:  
2 transmitting a close file request, along with the security object, from the  
3 distributed file system interface to the meta-data server, the close file request specifying  
4 the name of the first file;  
5 removing the encrypted block list of the first file from the security object.

1 6. The method of claim 5, further comprising returning the security object from  
2 the meta-data server to the distributed file system interface after removing the block  
3 list.

1 7. The method of claim 6, further comprising deleting the security object if there  
2 are no block lists in the security object after processing a close file request.

1 8. The method of claim 1, further comprising:  
2 encrypting file data at the distributed file interface for file write operations using  
3 the encryption key in the security object; and  
4 decrypting file data at the distributed file interface for file read operations using  
5 the encryption key in the security object.

1 9. The method of claim 1, further comprising:  
2 generating a partial encryption key at the meta-data server and storing the  
3 partial encryption key in the security object;  
4 transmitting the security object to the storage server; and

5 completing generation of the encryption key at the storage server using the  
6 partial encryption key and storing a complete encryption key in the security object; and  
7 returning the security object with the complete encryption key to the meta-data  
8 server.

1 10. The method of claim 1, further comprising:  
2 transmitting a close file request, along with the security object, from the  
3 distributed file system interface to the meta-data server, the close file request specifying  
4 the name of the first file;  
5 removing the encrypted block list of the first file from the security object.

1 11. The method of claim 10, further comprising returning the security object from  
2 the meta-data server to the distributed file system interface after removing the block  
3 list.

1 12. The method of claim 11, further comprising deleting the security object if there  
2 are no block lists in the security object after processing a close file request.

1 13. An apparatus for controlling access by a plurality of client applications to file  
2 data in a distributed file system including a distributed file system interface coupled to  
3 the client applications and a storage server and a meta-data server coupled to the  
4 distributed file system interface, comprising:

5 means for receiving at the meta-data server an open-file request, the open-file  
6 request specifying a name of a first file, wherein the first file includes a first set of  
7 blocks;

8 means for creating a security object at the meta-data server in response to the  
9 open-file request;

10 means for generating an encryption key at the meta-data server and the storage  
11 server and storing the encryption key in the security object;

12 means for encrypting a list that identifies the first set of blocks, whereby an  
13 encrypted block list is formed;

14 means for adding the encrypted block list to the security object; and

15 means for transmitting the security object to the distributed file interface.

1 14. A system for controlling access by a plurality of client applications to file data  
2 in a distributed file system, comprising:  
3 a distributed file system interface coupled to the client applications, the  
4 interface configured to transmit open file requests to a meta-data server and file access  
5 requests to a block storage server;  
6 the meta-data server coupled to the distributed file system interface and to the  
7 block storage server, the meta-data server configured to generate a partial encryption  
8 key, store the partial encryption key in a security object, transmit the security object to  
9 the block storage server for completion of the encryption key, encrypt a list of blocks in  
10 a file as an encrypted block list, and return the security object with the encrypted block  
11 list to the distributed file system interface; and  
12 the block storage server coupled to the distributed file system interface, the  
13 block storage server configured to generate a complete encryption key from the partial  
14 encryption key in the security object, and return the security object with the complete  
15 encryption key to the meta-data server.

1 15. The system of claim 14, wherein:  
2 the distributed file system interface is further configured to transmit a file access  
3 request and the security object to the block storage server in response to a file access  
4 request from a client application, the file access request including an operation code  
5 and a reference to selected data of a file; and  
6 the storage server is further configured to decrypt the encrypted block list in  
7 response to the file access request and provide access to the selected data in accordance  
8 with the operation code upon successful decryption of the block list.

1 16. The system of claim 14, wherein:  
2 the distributed file system interface is further configured to encrypt file data for  
3 file write operations using the encryption key in the security object decrypt file data for  
4 file read operations using the encryption key in the security object.